Easy LPEs and common software vulnerabilities

CHRISTOPHER VELLA

SECURITY RESEARCHER @ MICROSOFT

TWITTER: @KHAROSX0

Goal

Find 0-days fast

Hours / Days

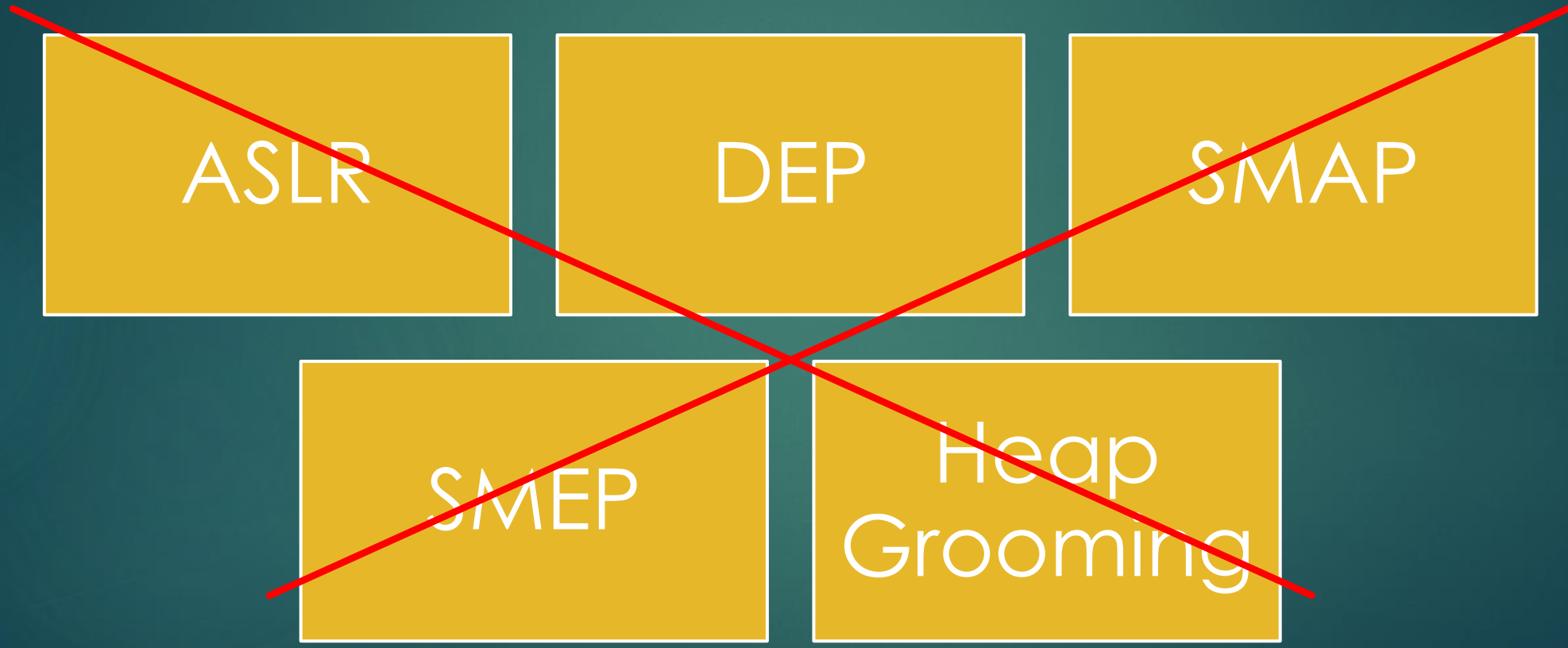
Easy to exploit

Bug -> LPE/RCE/SBX in a short time

Automation

As much as possible

Logic Vulns



Logic Vulns Cont.

```
hFile =
    CreateFile(
        "c:\\ProgramData\\MyFolder\\file1.txt"
        );
WriteFile(hFile, "test");
hFile2 =
    CreateFile(
        "c:\\ProgramData\\MyFolder\\file1.txt"
        );
WriteFile(hFile2, "test2");
```

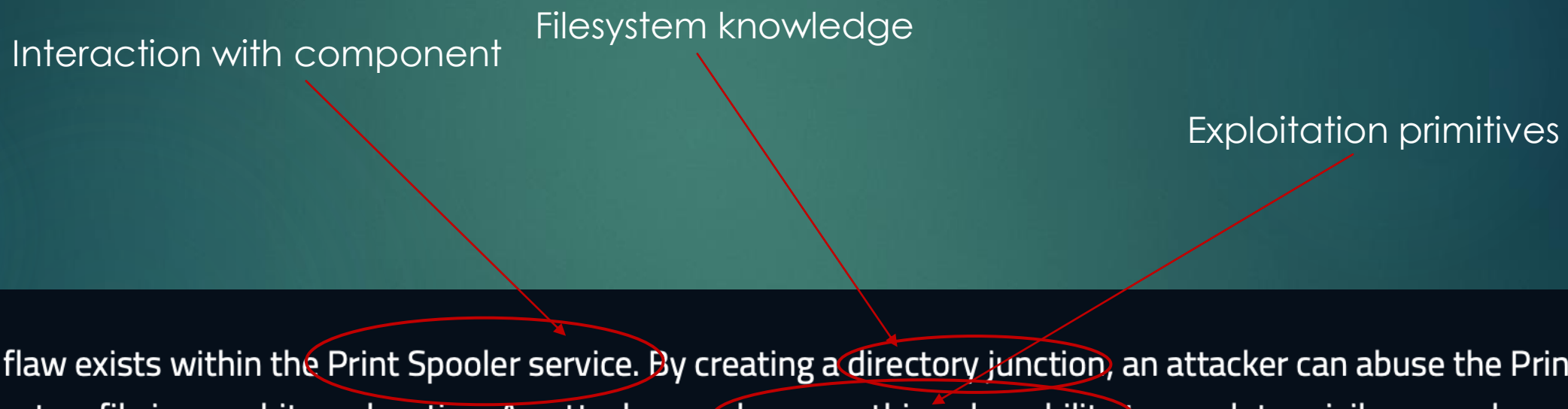
Various race conditions

Weak permission checks

Insufficient validation

Bad assumptions

What's in a 0-day



The specific flaw exists within the Print Spooler service. By creating a directory junction, an attacker can abuse the Print Spooler service to create a file in an arbitrary location. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of SYSTEM.

Common Attack Surfaces

- COM
- RPC
- Shared Memory
- Named Pipes
- File IO

Attack Surface Identification

- On Windows, plenty of tooling already built for you
- https://processhacker.sourceforge.io/
- https://github.com/hfiref0x/WinObjEx64
- https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite
- https://www.rpcview.org/
- https://github.com/googleprojectzero/sandbox-attacksurface-analysis-tools

File System Redirection

- “C:\Folder1\Folder2\File1.txt”

More info: See James Forshaw’s “A link to the past” talk ~2015

Not Unique to Windows

- MacOS & Linux have similar functionality
- Hard links can break assumptions when using certain APIs
- What if we had the follow hard link:
  - /temp/MyApp.app/Contents/MacOS/myexe -> /Applications/MyApp.app/Contents/MacOS/myexe

Instance Property

bundlePath

The full pathname of the receiver's bundle directory.

/Applications/MyApp.app

Junctions

- How common are junction related bugs?

ZDI-21-328	ZDI-CAN-12109	Microsoft	CVE-2021-26889	2021-03-17
Microsoft Windows Setup Directory Junction Privilege Escalation Vulnerability				
ZDI-21-327	ZDI-CAN-12108	Microsoft	CVE-2021-26886	2021-03-17
Microsoft Windows User Profile Service Directory Junction Denial-of-Service Vulnerability				
ZDI-21-286	ZDI-CAN-12442	Microsoft	CVE-2021-26866	2021-03-15
Microsoft Windows Update Agent Directory Junction Denial-of-Service Vulnerability				

Case Study: Zoom

Case Study: Foxit PDF Reader

Case Study: PuppetLabs

Case Study: Vmware Workstation

Takeaways

- Some vulnerability types are really easy to:
  - Identify, and
  - Exploit
- These also affect lots of software
  - Prominent third-party software
  - First-party software
- Not unique to Windows either

Future

- Certain bug classes have already been squashed in Windows
  - Like the fairly recent hard-link mitigations by Microsoft
  - C:\Windows\Temp mitigations are being tested
- Expect more mitigations to follow, at least in the Windows world